

# Quantum Error Correction of Observables

Cédric Bény,<sup>1</sup> Achim Kempf,<sup>1</sup> and David W. Kribs<sup>2,3</sup>

<sup>1</sup>*Department of Applied Mathematics,*

*University of Waterloo, ON, Canada, N2L 3G1*

<sup>2</sup>*Department of Mathematics and Statistics,*

*University of Guelph, Guelph, ON, Canada, N1G 2W1*

<sup>3</sup>*Institute for Quantum Computing, University of Waterloo, ON Canada, N2L 3G1*

(Dated: February 1, 2008)

A formalism for quantum error correction based on operator algebras was introduced in [1] via consideration of the Heisenberg picture for quantum dynamics. The resulting theory allows for the correction of hybrid quantum-classical information and does not require an encoded state to be entirely in one of the corresponding subspaces or subsystems. Here, we provide detailed proofs for the results of [1], derive a number of new results, and we elucidate key points with expanded discussions. We also present several examples and indicate how the theory can be extended to operator spaces and general positive operator-valued measures.

## I. INTRODUCTION

A new framework for quantum error correction was derived in [1] through a Heisenberg picture reformulation of the Schrödinger approach to error correction, and an expansion of the notion of a quantum code to allow for codes determined by algebras generated by observables. As the approach generalizes standard quantum error correction (QEC) [2, 3, 4, 5, 6] and operator quantum error correction (OQEC) [7, 8], we called the resulting theory “operator algebra quantum error correction” (OAQEC). An important feature of OAQEC is that it provides a formalism for the correction of hybrid quantum-classical information [9].

In this paper we provide proofs for the results stated in [1], and we establish a number of new results. In addition, we expose some of the finer points of the theory with discussions and several examples. We also outline how the theory can be extended to the case of operator spaces generated by observables and general positive operator-valued measures (POVMs).

We continue below by establishing notation and describing requisite preliminary notions.

In the next section we present a detailed analysis of passive quantum error correction within the OAQEC framework. The subsequent section does the same for active quantum error correction. This is followed by an expanded discussion of the application to information flow from [1], and we conclude with a section on the operator space and POVM extension.

### A. Preliminaries

Given a (finite-dimensional) Hilbert space  $\mathcal{H}$ , we let  $\mathcal{L}(\mathcal{H})$  be the set of operators on  $\mathcal{H}$  and let  $\mathcal{L}_1(\mathcal{H})$  be the set of density operators on  $\mathcal{H}$ . We shall write  $\rho, \sigma, \tau$  for density operators and  $X, Y$ , etc, for general operators. The identity operator will be written as  $\mathbf{1}$ .

Noise models in quantum computing are described (in the Schrödinger picture) by completely positive trace-preserving (CPTP) maps  $\mathcal{E} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H})$  [10]. We shall use the term *quantum channel* to describe such maps. Every map  $\mathcal{E}$  has an operator-sum representation  $\mathcal{E}(\rho) = \sum_a E_a \rho E_a^\dagger$ , where the operators  $E_a$  are called the *operation elements* or *noise operators* for  $\mathcal{E}$ . The Hilbert-Schmidt dual map  $\mathcal{E}^\dagger$  describes the corresponding evolution of observables in the Heisenberg picture. A set of operation elements for  $\mathcal{E}^\dagger$  is given by  $\{E_a^\dagger\}$ . Trace preservation of  $\mathcal{E}$  is equivalent to the requirement that  $\mathcal{E}^\dagger$  is *unital*; that is,  $\mathcal{E}^\dagger(\mathbf{1}) = \mathbf{1}$ .

A quantum system  $A$  (or  $B$ ) is a subsystem of  $\mathcal{H}$  if  $\mathcal{H}$  decomposes as  $\mathcal{H} = (A \otimes B) \oplus \mathcal{K}$ . Subspaces of  $\mathcal{H}$  can clearly be identified as subsystems  $A$  with one-dimensional ancilla ( $\dim B = 1$ ). An algebra  $\mathcal{A}$  of operators on  $\mathcal{H}$  that is closed under Hermitian conjugation is called a (finite-dimensional)  $C^*$ -algebra, what we will simply refer to as an “algebra”. Algebras of observables play a key role in quantum mechanics [11] and recently it has been shown that they can be used to encode hybrid quantum-classical information [9]. Below we shall discuss further the physical motivation for considering algebras in the present setting. Mathematically, finite-dimensional  $C^*$ -algebras have a tight structure theory that derives from their associated representation theory [12]. In particular, there is a decomposition of  $\mathcal{H}$  into subsystems  $\mathcal{H} = \bigoplus_k (A_k \otimes B_k) \oplus \mathcal{K}$  such that with respect to this decomposition the algebra is given by

$$\mathcal{A} = \left[ \bigoplus_k (\mathcal{L}(A_k) \otimes \mathbf{1}_{B_k}) \right] \bigoplus 0_{\mathcal{K}}. \quad (1)$$

The algebras  $\mathcal{L}(A_k) \otimes \mathbf{1}_{B_k}$  are referred to as the “simple” sectors of  $\mathcal{A}$ . We shall write  $\mathcal{M}_n$  for the set of  $n \times n$  complex matrices, and identify  $\mathcal{M}_n$  with the matrix representations for

elements of  $\mathcal{L}(A)$  when  $\dim A = n$  and an orthonormal basis for  $A$  is fixed.

## II. PASSIVE ERROR CORRECTION OF ALGEBRAS

As the terminology suggests, the existence of a passive code for a given noise model implies that no active operation is required (beyond decoding) to recover quantum information encoded therein. Mathematically, it is quite rare for a generic channel to have passive codes. However, many of the naturally arising physical noise models include symmetries that do allow for such codes [13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24].

The following is the standard definition of a noiseless subsystem (and decoherence-free subspace when  $\dim B = 1$ ) in the Schrödinger picture. Suppose we have a decomposition of the Hilbert space  $\mathcal{H}$  as  $\mathcal{H} = (A \otimes B) \oplus \mathcal{K}$ . As a notational convenience, we shall write  $\rho \otimes \tau$  for the operator on  $\mathcal{H}$  defined by  $(\rho \otimes \tau) \oplus 0_{\mathcal{K}}$ .

**Definition 1.** *We say that  $A$  is a noiseless (or decoherence-free) subsystem for  $\mathcal{E}$  if for all  $\rho \in \mathcal{L}_1(A)$  and  $\sigma \in \mathcal{L}_1(B)$  there exists  $\tau \in \mathcal{L}_1(B)$  such that*

$$\mathcal{E}(\rho \otimes \sigma) = \rho \otimes \tau. \quad (2)$$

The “decoherence-free” terminology is usually reserved for subspaces (when  $\dim B = 1$ ).

### A. Decoherence-Free And Noiseless Subspaces And Subsystems In The Heisenberg Picture

The following theorem gives an equivalent formulation of this definition in the Heisenberg picture, that is in terms of the evolution of observables, given by the dual channel  $\mathcal{E}^\dagger$ . We introduce the projector  $P$  of  $\mathcal{H}$  onto the subspace  $A \otimes B$ .

**Theorem 2.**  *$A$  is a noiseless subsystem for  $\mathcal{E}$  if and only if*

$$P \mathcal{E}^\dagger(X \otimes \mathbf{1}) P = X \otimes \mathbf{1} \quad (3)$$

*for all operators  $X \in \mathcal{L}(A)$*

**Proof.** If  $A$  is a noiseless subsystem for  $\mathcal{E}$ , then for all  $X \in \mathcal{L}(A)$  we have

$$\begin{aligned} \text{Tr}(P\mathcal{E}^\dagger(X \otimes \mathbf{1})P(\rho \otimes \sigma)) &= \text{Tr}(\mathcal{E}^\dagger(X \otimes \mathbf{1})(\rho \otimes \sigma)) = \text{Tr}((X \otimes \mathbf{1})\mathcal{E}(\rho \otimes \sigma)) \\ &= \text{Tr}(X\rho \otimes \tau) = \text{Tr}(X\rho)\text{Tr}(\tau) \\ &= \text{Tr}(X\rho) = \text{Tr}((X \otimes \mathbf{1})(\rho \otimes \sigma)). \end{aligned}$$

This is true for all  $\rho \in \mathcal{L}_1(A)$  and all  $\sigma \in \mathcal{L}_1(B)$ . By linearity it follows that  $P\mathcal{E}^\dagger(X \otimes \mathbf{1})P = X \otimes \mathbf{1}$  for all  $X \in \mathcal{L}(A)$ .

Reciprocally, if we assume Eq. (3) to be true for all  $X \in \mathcal{L}(A)$ , then for all  $\gamma \in \mathcal{L}_1(A \otimes B)$  we have

$$\begin{aligned} \text{Tr}(X \text{Tr}_B(P\mathcal{E}(\gamma)P)) &= \text{Tr}((X \otimes \mathbf{1})P\mathcal{E}(\gamma)P) = \text{Tr}(P\mathcal{E}^\dagger(X \otimes \mathbf{1})P\gamma) \\ &= \text{Tr}((X \otimes \mathbf{1})\gamma) = \text{Tr}(X \text{Tr}_B(\gamma)), \end{aligned}$$

where we have freely used the facts  $P(X \otimes \mathbf{1})P = X \otimes \mathbf{1}$  and  $P\gamma P = \gamma$ . Since the above equation is true for all  $X$ , we have  $\text{Tr}_B(P\mathcal{E}(\gamma)P) = \text{Tr}_B(\gamma)$  for all  $\gamma \in \mathcal{L}_1(A \otimes B)$ , which was shown in [8] to be equivalent to the definition of  $A$  being a noiseless subsystem for  $\mathcal{E}$ .  $\square$

Note that Eq. (3) can be satisfied even if part of an observable  $X \otimes \mathbf{1}$  spills outside of the subspace  $P\mathcal{H}$  under the action of  $\mathcal{E}^\dagger$ . The projectors  $P$  in Eq. (3) show that the noiseless subsystem condition in the Heisenberg picture is only concerned with the “matrix corner” of  $\mathcal{E}^\dagger(X \otimes \mathbf{1})$  partitioned by  $P$ .

In some cases the equivalence of Eq. (2) and Eq. (3) can be seen from a different perspective. For a bistochastic or unital channel (those for which  $\mathcal{E}(\mathbf{1}) = \mathbf{1}$ ), the dual  $\mathcal{E}^\dagger$  is also a channel. Then structural results for unital channels from [26] can be used to give an alternate realization of this equivalence, and passive codes may be computed directly from the commutant of the operation elements for  $\mathcal{E}$ . The simplest case would be for “self-dual” channels, those for which  $\mathcal{E}^\dagger = \mathcal{E}$ . Clearly, any  $\mathcal{E}$  with Hermitian operation elements is self-dual. In particular, self-dual channels include all Pauli noise models, which are channels with operation elements belonging to the Pauli group, the group generated by tensor products of unitary Pauli operators  $X, Y, Z$ .

As a further illustrative (non-unital) example, consider the single-qubit spontaneous emission channel [10] given by  $\mathcal{E}(\sigma) = \text{Tr}(\sigma)|0\rangle\langle 0|$ . Here  $P = |0\rangle\langle 0|$ . This channel is

implemented by operation elements  $E_0 = P$  and  $E_1 = |0\rangle\langle 1|$ . Hence the dual channel is given by  $\mathcal{E}^\dagger(\sigma) = P\sigma P + E_1^\dagger\sigma E_1$ . The subspace  $A$  spanned by the ground state  $|0\rangle$  is a decoherence-free subspace for  $\mathcal{E}$  (though it cannot be used to encode quantum information since  $\dim A = 1$ ). In this case, Eq. (3) is equivalent to the statement  $P\mathcal{E}^\dagger(P)P = P$ , which may be readily verified.

One can consider more general spontaneous emission channels with non-trivial decoherence-free subspaces. For instance, consider a qutrit noise model that describes spontaneous emission from the second excited state to the ground state. The corresponding channel is defined by  $\mathcal{E}(\sigma) = P\sigma P + E\sigma E^\dagger$ , where  $P = |0\rangle\langle 0| + |1\rangle\langle 1|$  and  $E = |0\rangle\langle 2|$ . The subspace  $P\mathbb{C}^3 = \text{span}\{|0\rangle, |1\rangle\}$  is a single-qubit decoherence-free subspace for  $\mathcal{E}$  since  $\mathcal{E}(\sigma) = \sigma$  for all  $\sigma = P\sigma P$ . It is also easy to see in this case that Eq. (3) is satisfied since  $P\mathcal{E}^\dagger(X)P = X$  for all  $X \in \mathcal{L}(P\mathbb{C}^3)$ . Notice also in this example that  $\mathcal{E}^\dagger$  can induce “spillage” from  $P$  to  $P^\perp$ . Indeed, this can be seen immediately from the operator-sum representation for  $\mathcal{E}^\dagger$ ; specifically, for all  $X \in \mathcal{L}(P\mathbb{C}^3)$  we have

$$\mathcal{E}^\dagger(X) = PXP + E^\dagger X E = X + \alpha |2\rangle\langle 2|, \quad (4)$$

where  $\alpha = \langle 0|X|0\rangle$ .

## B. Conserved Algebras Of Observables

A POVM determined by a set of operators  $X = \{X_a\}$  evolves via the unital CP-map  $\mathcal{E}^\dagger$  in the Heisenberg picture. If for all  $a$  we have  $X_a = \mathcal{E}^\dagger(X_a)$ , then all the statistical information about  $X = \{X_a\}$  has been conserved. Indeed, for any initial state  $\rho$ , we have  $\text{Tr}(\rho X_a) = \text{Tr}(\rho \mathcal{E}^\dagger(X_a)) = \text{Tr}(\mathcal{E}(\rho) X_a)$ . Moreover, if we have control on the initial states, an expected feature in quantum computing, we can ask which elements are conserved if the state starts in a certain subspace  $P\mathcal{H}$ ; that is, which elements satisfy  $P\mathcal{E}^\dagger(X_a)P = PX_aP$ , or equivalently  $\text{Tr}(X_a \mathcal{E}(P\rho P)) = \text{Tr}(X_a P\rho P)$  for all  $\rho \in \mathcal{L}_1(\mathcal{H})$ . This, together with the Heisenberg characterization of Eq. (3), motivates the following definition.

**Definition 3.** *We shall say that a set  $\mathcal{S}$  of operators on  $\mathcal{H}$  is conserved by  $\mathcal{E}$  for states in  $P\mathcal{H}$  if every element of  $\mathcal{S}$  is conserved; that is, if*

$$P\mathcal{E}^\dagger(X)P = PX P \quad \forall X \in \mathcal{S}. \quad (5)$$

The focus of the present work is error correction for algebras generated by observables. Let us consider in more detail the physical motivation for considering algebras. In the Heisenberg picture a set of operators  $\{X_a\}$  evolves according to the unital CP-map  $\mathcal{E}^\dagger$  with elements  $E_a^\dagger$  instead of  $E_a$ . If for all values of the label  $a$  we have  $X_a = \mathcal{E}^\dagger(X_a)$  then all the statistical information about  $X$  has been conserved by  $\mathcal{E}$  as noted above. In such a scenario we say that  $X_a$  is conserved by  $\mathcal{E}$ . In particular, if  $X$  defines a standard projective measurement,  $X = \sum_a p_a X_a$  with  $X_a^2 = X_a$  for all  $a$ , then the projectors  $X_a$  linearly span the algebra they generate. Hence, in this case  $\mathcal{E}$  conserves an entire commutative algebra. Therefore, focussing on the conservation (and more generally correction defined later) of sets of operators that have the structure of an algebra, apart from allowing a complete characterization, is also sufficient for the study of all the correctable *projective* observables.

Further observe that Eq. (5) applied to a set of observables that generate an (arbitrary) algebra gives a generalization of noiseless subsystems. Indeed, by Theorem 2 any subalgebra  $\mathcal{A}$  of  $\mathcal{L}(P\mathcal{H})$  for which all elements  $X \in \mathcal{A}$  satisfy Eq. (5) is a direct sum of simple algebras, each of which encodes a noiseless subsystem (when  $\dim A_k > 1$  as in Eq. (1)). It is also important to note that given an algebra  $\mathcal{A}$  conserved for states in  $P\mathcal{H}$  (or more generally correctable as we shall see) quantum information cannot in general be encoded into the entire subspace  $P\mathcal{H}$  for safe recovery, but rather into subsystems of  $P\mathcal{H}$  determined by the splitting induced from the algebra structure of  $\mathcal{A}$ . These points will be further expanded upon in the discussion of Section III B.

We now establish concrete testable conditions for passive error correction. Namely, these conditions are stated strictly in terms of the operation elements for a channel. This result was stated without proof in [1]. The special case of simple algebras in the Schrödinger picture was obtained in [7, 8]. Techniques of [23] are used in the analysis. We first present a simple lemma that will be used below.

**Lemma 4.** *Let  $\mathcal{F}$  be a CP map with elements  $F_a$ . If  $A \geq 0$  is such that  $\mathcal{F}(A) = 0$  then it follows that  $AF_a = 0$  for every element  $F_a$ .*

**Proof.** If  $\sum_a F_a^\dagger A F_a = 0$  then for any state  $|\psi\rangle$ ,  $\sum_a \langle\psi|F_a^\dagger A F_a|\psi\rangle = 0$ . Since each operator  $F_a^\dagger A F_a$  is positive, this is a sum of nonnegative terms. Therefore each individual term must equal zero;  $\langle\psi|F_a^\dagger A F_a|\psi\rangle = 0$  for all  $a$ . This means that the vector  $\sqrt{A}F_a|\psi\rangle$  is of norm zero, and therefore is the zero vector. This being true for all states  $|\psi\rangle$ , we must have that

$\sqrt{A}F_a = 0$ , from which it follows that  $AF_a = 0$ .  $\square$

**Theorem 5.** *Let  $\mathcal{A}$  be a subalgebra of  $\mathcal{L}(P\mathcal{H})$ . The following statements are equivalent:*

1.  $\mathcal{A}$  is conserved by  $\mathcal{E}$  for states in  $P\mathcal{H}$ .
2.  $[E_a P, X] = 0$  for all  $X \in \mathcal{A}$  and all  $a$ .

**Proof.** If  $[E_a P, X] = [E_a P, PXP] = 0$  for all  $a$ , then

$$\begin{aligned} P\mathcal{E}^\dagger(X)P &= \sum_a PE_a^\dagger X E_a P = \sum_a PE_a^\dagger PXP E_a P \\ &= \sum_a PE_a^\dagger E_a PXP = P\mathcal{E}^\dagger(\mathbf{1})PXP = PXP = X. \end{aligned}$$

Reciprocally, we assume that each  $X \in \mathcal{A}$  satisfies  $P\mathcal{E}^\dagger(X)P = PXP = X$ . Consider a projector  $Q \in \mathcal{A}$ . We have  $P\mathcal{E}^\dagger(Q)P = Q$  and hence  $P\mathcal{E}^\dagger(Q^\perp)P = PQ^\perp$ . Therefore

$$Q^\perp P\mathcal{E}^\dagger(Q)PQ^\perp = Q^\perp Q Q^\perp = 0,$$

and similarly  $Q P\mathcal{E}^\dagger(Q^\perp)PQ = 0$ . By Lemma 4, this implies respectively  $QE_a P Q^\perp = 0$  and  $Q^\perp E_a P Q = 0$  for all  $a$ . Together these conditions imply

$$QE_a P = QE_a P Q = E_a P Q,$$

and thus  $[E_a P, Q] = 0$  for all  $a$ . Finally, note that since  $\mathcal{A}$  is an algebra, then a generic element  $Y \in \mathcal{A}$  can be written as a linear combination of projectors in  $\mathcal{A}$ . Therefore we also have  $[E_a P, Y] = 0$  for all  $Y \in \mathcal{A}$ , and this completes the proof.  $\square$

This theorem allows us to identify the largest conserved subalgebra of  $\mathcal{L}(P\mathcal{H})$  conserved on the subspace  $P\mathcal{H}$ . Namely, a direct consequence of Theorem 5 is that the (necessarily  $\dagger$ -closed) commutant inside  $\mathcal{L}(P\mathcal{H})$  of the operators  $\{E_a P, PE_a^\dagger\}$  is the largest such algebra.

**Corollary 6.** *The algebra  $\mathcal{A} = \{X \in \mathcal{L}(P\mathcal{H}) : \forall a [X, E_a P] = [X^\dagger, E_a P] = 0\}$  is conserved on states in  $P\mathcal{H}$  and contains all subalgebras of  $\mathcal{L}(P\mathcal{H})$  conserved on states  $P\mathcal{H}$ .*

Note that  $P$  itself may not belong to this algebra, unless it satisfies  $E_a P = PE_a P$ . This special case was the case considered in [23]. With other motivations in mind, the special case  $P = \mathbf{1}$  was also derived in [25] where it was shown that the full commutant of  $\{E_a, E_a^\dagger\}$  is the largest algebra inside the fixed point set of a unital CP map. (This in turn may be regarded as a weaker form of the fixed point theorem for unital channels [26].)

Likely the most prevalent class of decoherence-free subspaces are the stabilizer subspaces for abelian Pauli groups, which give the starting point for the stabilizer formalism [6]. On the  $n$ -qubit Hilbert space, let  $s < n$  and consider the group  $S$  generated by the Pauli phase flip operators  $Z_1, \dots, Z_s$ , where we have written  $Z_1 = Z \otimes \mathbf{1} \otimes \dots \otimes \mathbf{1}$ , etc. The joint eigenvalue-1 space for  $S$  is a  $2^{n-s}$ -dimensional decoherence-free subspace for  $\{Z_j : 1 \leq j \leq s\}$ , called the “stabilizer subspace” for  $S$ . In the stabilizer formalism, any of the  $2^s$  (necessarily  $2^{n-s}$ -dimensional) mutually orthogonal joint eigenspaces for elements of  $S$  could be used individually to build codes, but the eigenvalue-1 space is used as a convenience. Each of these eigenspaces supports a full matrix algebra  $\mathcal{M}_k$ , where  $k = 2^{n-s}$ . In the present setting these decoherence-free subspaces may be considered together, as they are defined by the structure of the commutant  $S' \cong \mathcal{M}_k^{(2^s)}$ . In particular, this entire algebra is conserved by any channel defined with operation elements given by linear combinations of elements taken from  $S$ .

Allowing other Pauli operators into the error group can result in non-conserved scenarios. For instance, consider the case  $n = 3$  and  $s = 2$ . The algebra  $S' \cong \mathcal{M}_2^{(4)}$  is conserved by channels determined by elements of  $S$  as above. However, it is *not* conserved by channels determined by elements of  $G = \{Z_1, Z_2, X_1 X_2\}$ , even though the individual eigenvalue-1 stabilizer space is still a correctable code for  $G$ . This follows from Theorem 5 since  $G$  properly contains  $S$ , and hence  $G'$  is properly contained in  $S'$ . (In this case  $P = \mathbf{1}$ , and the largest conserved algebra is the full commutant  $G'$  of the error group.) Interestingly, there are still algebras conserved by channels determined by elements of  $G$ , since its commutant has the structure  $G' = \text{Alg}\{G\}' \cong (I_2 \otimes \mathcal{M}_2) \oplus (I_2 \otimes \mathcal{M}_2)$ .

Let us reconsider the special case in which the projector  $P$  itself is one of the correctable observables. Most importantly, this guarantees that after evolution all states are back into the code  $P\mathcal{H}$ . Indeed, the probability that a state  $\rho$  initially in the code is still in the code after evolution is then given by

$$p = \text{Tr}(\mathcal{E}(\rho)P) = \text{Tr}(\rho P \mathcal{E}^\dagger(P)P) = \text{Tr}(\rho P) = 1. \quad (6)$$

We note that this also guarantees a repetition of the noise map will be conserved.

A refinement of the proof of Theorem 5 yields the following result when the projector  $P$



is conserved and belongs to the algebra of observables in question.

**Theorem 7.** *Let  $\mathcal{A}$  be an algebra containing the projector  $P$ . The following statements are equivalent:*

1.  $\mathcal{A}$  is conserved by  $\mathcal{E}$  for states in  $P\mathcal{H}$ .
2.  $[E_a P, X] = 0$  for all  $X \in P\mathcal{A}P$  and all  $a$ .

**Proof.** If  $[E_a P, X] = [E_a P, PXP] = 0$  for all  $a$ , then  $P\mathcal{E}^\dagger(X)P = PXP$  follows as above. On the other hand, if each  $X \in \mathcal{A}$  satisfies  $P\mathcal{E}^\dagger(X)P = PXP$ , then note that for  $X = P$  this yields  $P\mathcal{E}^\dagger(P)P = P$  which implies  $P\mathcal{E}^\dagger(P^\perp)P = 0$ . Therefore, by Lemma 4,  $P^\perp E_a P = 0$ , that is,  $E_a P = P E_a P$  for all  $a$ . Hence for all  $X \in \mathcal{A}$  we also have  $P\mathcal{E}^\dagger(PXP)P = PXP$ . But the set  $P\mathcal{A}P$  is itself an algebra, since  $P$  belongs to  $\mathcal{A}$ , and hence is spanned by its projectors. The rest of the proof proceeds as above.  $\square$

### III. ACTIVE ERROR CORRECTION OF ALGEBRAS

More generally, active intervention into a quantum system may be required for error correction. In particular, we should be able to protect a set of operators  $\{X_a\}$  (which could define a POVM for instance) by acting with a channel  $\mathcal{R}$  such that each  $X_a$  is mapped by  $\mathcal{R}^\dagger$  to one of the operators  $Y_a = \mathcal{E}^\dagger(X_a)$ . That is,  $\mathcal{R}^\dagger(X_a) = Y_a$ , and thus  $(\mathcal{R} \circ \mathcal{E})^\dagger(X_a) = X_a$ . This, together with the previous discussions, motivates the following definition.

**Definition 8.** *We say that a set  $\mathcal{S}$  of operators on  $\mathcal{H}$  is correctable for  $\mathcal{E}$  on states in the subspace  $P\mathcal{H}$  if there exists a channel  $\mathcal{R}$  such that  $\mathcal{S}$  is conserved by  $\mathcal{R} \circ \mathcal{E}$  on states in  $P\mathcal{H}$ ; in other words,*

$$P(\mathcal{R} \circ \mathcal{E})^\dagger(X)P = PXP \quad \forall X \in \mathcal{S}. \quad (7)$$

This equation is the same as the one we used to defined passive error correction, except that we now allow for an arbitrary “correction operation”  $\mathcal{R}$  after the channel has acted. In particular, as in other settings, the passive case may be regarded as the special case of active error correction for which the correction operation is trivial,  $\mathcal{R} = \text{id}$ .

This notion of correctability is more general than the one addressed by the framework of OQEC, and extends the one introduced in [1] from algebras to arbitrary sets of observables. Here we shall continue to focus on algebras, and in Section V we consider an extension of the

notion to general operator spaces. Whereas OQEC focusses on simple algebras,  $\mathcal{L}(A) \otimes \mathbf{1}^B$ , here correctability is defined for any set, and in particular for any finite-dimensional algebra. See Section IIIB for an expanded discussion on the form of OAQEC codes.

### A. Testable Conditions For OAQEC Codes

A set of operation elements for a given channel are the fundamental building blocks for the associated physical noise model. Thus, a characterization of a correctable OAQEC code strictly in terms of the operation elements for a given channel is of immediate interest. The following result was stated without proof in [1]. It generalizes the central result for both QEC [3] and OQEC [7, 8, 28].

**Theorem 9.** *Let  $\mathcal{A}$  be a subalgebra of  $\mathcal{L}(P\mathcal{H})$ . The following statements are equivalent:*

1.  $\mathcal{A}$  is correctable for  $\mathcal{E}$  on states in  $P\mathcal{H}$ .
2.  $[PE_a^\dagger E_b P, X] = 0$  for all  $X \in \mathcal{A}$  and all  $a, b$ .

**Proof.** We write  $R_a$  for the elements of  $\mathcal{R}$ . According to Theorem 5, the conservation of  $\mathcal{A}$  by  $\mathcal{R} \circ \mathcal{E}$  implies  $R_a E_b X = X R_a E_b P$  for all  $X \in \mathcal{A}$  and all  $a, b$ . But we also have  $R_a E_b X^\dagger = X^\dagger R_a E_b P$ , so that  $X E_b^\dagger R_a^\dagger = P E_b^\dagger R_a^\dagger X$ . Therefore  $PE_c^\dagger E_b X = \sum_a PE_c^\dagger R_a^\dagger R_a E_b X = \sum_a PE_c^\dagger R_a^\dagger X R_a E_b P = X E_c^\dagger E_b P$ .

We will prove the sufficiency of this condition by explicitly constructing a correction channel. For  $k \geq 1$ , let  $P_k$  be the projector onto the  $k$ th simple sector of the algebra  $\mathcal{A}$ . Also let  $P_0 = P - \mathbf{1}_{\mathcal{A}}$  where  $\mathbf{1}_{\mathcal{A}}$  is the unit element of the algebra  $\mathcal{A}$ . We have  $P_k E_b^\dagger E_c P_k = \mathbf{1} \otimes A_{bc}$  for some operators  $A_{bc}$  and all  $k \geq 0$ . Hence the theory of operator error correction guarantees that each subspace can be individually corrected. Here however we have the additional property  $P_k E_b^\dagger E_c P_{k'} = 0$  whenever  $k \neq k'$ , which allows the correction of the state even if it is in a superposition between several of the subspaces  $P_k$ . Explicitly, we have  $(\mathbf{1} \otimes \langle l |) P_k (E_b^\dagger E_c) P_{k'} (\mathbf{1} \otimes | l' \rangle) = \delta_{kk'} \lambda_{bc}^{kll'} \mathbf{1}$  for some  $\lambda_{bc}^{kll'} \in \mathbb{C}$ , where we denote  $\mathbf{1} = \mathbf{1}_{m_k}$ . According to the standard theory of error correction this condition guarantees the existence of channels  $\mathcal{R}_k$  correcting the error operators  $F_{ckl} = E_c P_k (\mathbf{1} \otimes | l \rangle)$  for all  $l$  and all  $c$ , or any linear combination of them. In particular, we will consider linear combinations of the form  $\tilde{F}_{ck} = \sum_n \langle n | \psi \rangle F_{ckn} = E_c P_k (\mathbf{1} \otimes | \psi \rangle)$  for any normalized vector  $|\psi\rangle$ . Furthermore, from the

standard theory we know the elements of the correction channels  $\mathcal{R}_k$  can be assumed to have the form  $R_{cl}^{(k)} = \sum_{bj} \alpha_{clbj}^{(k)} (\mathbf{1} \otimes \langle j|) P_k E_b^\dagger$  for some complex numbers  $\alpha_{clbj}^{(k)}$ .

We now show that the trace-decreasing channel  $\mathcal{R}$  with elements  $R_{kcl} = P_k (\mathbf{1} \otimes |l\rangle) R_{cl}^{(k)}$  corrects the algebra  $\mathcal{A}$  on states  $P\mathcal{H}$  for the channel  $\mathcal{E}$ . First note that  $R_{cl}^{(k)} E_a P = \sum_{bj} \alpha_{clbj}^{(k)} (\mathbf{1} \otimes \langle j|) P_k E_b^\dagger E_a P_k = R_{cl}^{(k)} E_a P_k$ . Hence, for a general operator  $X = \sum_k A_k \otimes \mathbf{1}$  in the algebra we have  $P(\mathcal{E}^\dagger \circ \mathcal{R}^\dagger)(X)P = \sum_{ackl} P_k E_c^\dagger R_{al}^{(k)\dagger} A_k R_{al}^{(k)} E_c P_k$ . Considering each term  $k$  separately, for any state  $|\psi\rangle$  we have

$$\begin{aligned} & \sum_{acl} (\mathbf{1} \otimes \langle \psi|) P_k E_c^\dagger R_{al}^{(k)\dagger} A_k R_{al}^{(k)} E_c P_k (\mathbf{1} \otimes |\psi\rangle) \\ &= A_k = (\mathbf{1} \otimes \langle \psi|) (A_k \otimes \mathbf{1}) (\mathbf{1} \otimes |\psi\rangle), \end{aligned}$$

where we have used the dual of the fact that  $\mathcal{R}_k$  corrects the error operators  $\tilde{F}_{ck}$ . Therefore  $\sum_{acl} P_k E_c^\dagger R_{al}^{(k)\dagger} A_k R_{al}^{(k)} E_c P_k = (A_k \otimes \mathbf{1})$  and summing those terms over  $k$  yields  $P(\mathcal{E}^\dagger \circ \mathcal{R}^\dagger)(X)P = \sum_k (A_k \otimes \mathbf{1}) = X$ .  $\square$

As an immediate consequence of Theorem 9 we have the following.

**Corollary 10.** *The algebra  $\mathcal{A} = \{X \in \mathcal{L}(P\mathcal{H}) : \forall a, b [X, P E_a^\dagger E_b P] = 0\}$  is correctable on states in  $P\mathcal{H}$  and contains all subalgebras of  $\mathcal{L}(P\mathcal{H})$  correctable on states in  $P\mathcal{H}$ .*

To further explain the structure of the correction channel in Theorem 9 let us show how it is constructed from OQEC correction channels. This will also give an alternative proof of the sufficiency of the correctability condition.

For simplicity, we will in fact build a channel which corrects the larger algebra  $\mathcal{B} := \mathcal{A} \oplus \mathbb{C}(\mathbf{1}_{\mathcal{A}} - P)$ . Remember that  $P_k$  is the projector onto the  $k$ th simple sector of the algebra  $\mathcal{A}$ , assuming a decomposition as in Eq. (1). Also we include  $P_0 = \mathbf{1}_{\mathcal{A}} - P$  which projects onto the additional sector in  $\mathcal{B}$ . Our correctability condition guarantees that each of those sectors is an OQEC code. Let  $\mathcal{R}_k$  be a OQEC correction channel for the  $k$ th simple sector. We use the “raw” subunitary version of the subsystem correction channels whose elements are all linear combinations of the operators  $P_k E_a^\dagger$ . They have the property that  $Q_k := \mathcal{R}_k^\dagger(\mathbf{1}) = \mathcal{R}_k^\dagger(P_k)$  is a projector. Since the elements of the channel  $\mathcal{R}_k$  are linear combinations of the operators  $P_k E_a^\dagger$ , we have  $Q_k Q_l = \mathcal{R}_k^\dagger(P_k) \mathcal{R}_l^\dagger(P_l) = 0$  if  $k \neq l$ , because all the terms contain a factor of the form  $P_k E_a^\dagger E_b P_l = 0$ . This means the projectors  $Q_k$  are mutually orthogonal and sum to a projector  $Q := \sum_k Q_k$ . The channels  $\mathcal{R}_k$  also have

the property that  $\mathcal{R}_k(\rho) = \mathcal{R}_k(Q_k \rho Q_k)$  for any state  $\rho$ . From these “local” channels we can construct a trace-preserving correction channel for the full algebra:

$$\mathcal{R}^\dagger(X) := \sum_k \mathcal{R}_k^\dagger(X) + \frac{\text{Tr}(PX)}{\text{Tr}(P)} Q^\perp \quad (8)$$

This CP map is a channel because  $\mathcal{R}^\dagger(\mathbf{1}) = \sum_k Q_k + Q^\perp = \mathbf{1}$ . We have to check that it corrects the algebra  $\mathcal{B}$ . First, concerning the effect of  $\mathcal{E}^\dagger$  on the last term of the correction channel, note that

$$\begin{aligned} P\mathcal{E}^\dagger(Q)P &= \sum_k P\mathcal{E}^\dagger(\mathcal{R}_k^\dagger(P_k))P \\ &= \sum_k P_k \mathcal{E}^\dagger(\mathcal{R}_k^\dagger(P_k))P_k = \sum_k P_k = P. \end{aligned}$$

Hence  $P\mathcal{E}^\dagger(Q^\perp)P = 0$ . It follows that for any  $X \in \mathcal{B}$  we have, keeping in mind that the channel elements of  $\mathcal{R}_k$  are linear combinations of the operators  $P_k E_a^\dagger$ ,

$$\begin{aligned} P\mathcal{E}^\dagger(\mathcal{R}^\dagger(X))P &= \sum_{kl} P_l \mathcal{E}^\dagger(\mathcal{R}_k^\dagger(X))P_l \\ &= \sum_k P_k \mathcal{E}^\dagger(\mathcal{R}_k^\dagger(X))P_k \\ &= \sum_k P_k X P_k = X, \end{aligned}$$

which is the desired property for the correction channel  $\mathcal{R}$ .

As in the passive case, we can consider the situation in which the projector is correctable and belongs to the algebra. In this case, the observables and states do not spill out from  $P\mathcal{H}$  under the action of  $\mathcal{R} \circ \mathcal{E}$ , and so the channel followed by the correction operation is repeatable. The previous proof can be readily refined for this purpose.

**Theorem 11.** *Let  $\mathcal{A}$  be an algebra containing the projector  $P$ . The following statements are equivalent:*

1.  $\mathcal{A}$  is correctable for  $\mathcal{E}$  on states in  $P\mathcal{H}$ .
2.  $[PE_a^\dagger E_b P, X] = 0$  for all  $X \in P\mathcal{A}P$  and all  $a, b$ .

**Proof.** Since  $P \in \mathcal{A}$  then  $P\mathcal{A}P$  is a subalgebra of  $\mathcal{A}$ . Therefore correctability of  $\mathcal{A}$  implies correctability of  $P\mathcal{A}P$  which from Theorem 9 implies that  $[PE_a^\dagger E_b P, X] = 0$  for all  $X \in P\mathcal{A}P$ . Reciprocally, if this condition is satisfied then by Theorem 9 there exists

a channel  $\mathcal{R}$  correcting the algebra  $P\mathcal{A}P$ . In fact this channel corrects all of  $\mathcal{A}$ . Indeed, remember that the channel  $\mathcal{R}$  built in the proof is such that  $\mathcal{R}^\dagger(X) = \mathcal{R}^\dagger(PXP)$  for all  $X$ . Therefore for all  $X \in \mathcal{A}$ ,  $P(\mathcal{R} \circ \mathcal{E})^\dagger(X)P = P(\mathcal{R} \circ \mathcal{E})^\dagger(PXP)P = PXP$ .  $\square$

In practice, the operation elements for a channel are usually not known precisely; often it is just the linear space they span that is known [27]. Thus, for the explicit construction of correction operations in Theorems 9 and 11 to be of practical value, one has to show that the correction channel  $\mathcal{R}$  also corrects any channel whose elements are linear combinations of the elements  $E_a$ . This is indeed the case. A simple way to see this is to note that if the testable conditions for conserved algebras of Theorems 5 and 7 are satisfied for  $\mathcal{R} \circ \mathcal{E}$ , then they are also satisfied for  $\mathcal{R} \circ \mathcal{E}'$  where the operation elements of  $\mathcal{E}'$  are linear combinations of those for  $\mathcal{E}$ .

## B. The Schrödinger Picture

In order to illustrate how OAQEC generalizes OQEC we restate a special case of the above results in the Schrödinger picture: Suppose we have a decomposition

$$\mathcal{H} = \left[ \bigoplus_k (A_k \otimes B_k) \right] \oplus \mathcal{K}, \quad (9)$$

with  $P$  the projector of  $\mathcal{H}$  onto  $\mathcal{K}^\perp = \bigoplus_k A_k \otimes B_k$ . The algebra in question includes  $P$  as its unit and is given by  $\mathcal{A} = \left[ \bigoplus_k (\mathcal{L}(A_k) \otimes \mathbf{1}_{B_k}) \right] \oplus 0_{\mathcal{K}}$ . Observe that the hypotheses of both results Theorems 9 and 11 are satisfied. It follows that  $\mathcal{A}$  is correctable for  $\mathcal{E}$  for states in  $P\mathcal{H}$  if and only if there exists a channel  $\mathcal{R}$  such that for any density operator  $\rho = \sum_k \alpha_k (\rho_k \otimes \tau_k)$  with  $\rho_k \in \mathcal{L}_1(A_k)$ ,  $\tau_k \in \mathcal{L}_1(B_k)$ , and nonnegative scalars  $\sum_k \alpha_k = 1$ , there are operators  $\tau'_k \in \mathcal{L}_1(B_k)$  for which

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \sum_k \alpha_k \mathcal{R}(\mathcal{E}(\rho_k \otimes \tau_k)) = \sum_k \alpha_k (\rho_k \otimes \tau'_k). \quad (10)$$

Experimentally, each of the subsystems  $A_k$  can be used individually to encode quantum information. An extra feature of this OAQEC code is the fact that an arbitrary mixture of encoded states, one for each subsystem, can be simultaneously corrected by the same correction operation.

By Theorem 9 (or Theorem 11), there is a correction operation  $\mathcal{R}$  for which Eq. (10) is

satisfied if and only if for all  $a, b$  there are operators  $X_{abk} \in \mathcal{L}(B_k)$  such that

$$PE_a^\dagger E_b P = \sum_k \mathbf{1}_{A_k} \otimes X_{abk}. \quad (11)$$

Note that contrary to the Heisenberg formulation of Eq. (7), the formulation of Eq. (10) implicitly relies on the representation theory for finite-dimensional  $C^*$ -algebras. As the representation theory for arbitrary  $C^*$ -algebras is intractable, this suggests the Heisenberg picture may be more appropriate for an infinite-dimensional generalization of this framework.

Let us consider a qubit-based class of examples to illustrate the equivalence established in Theorem 9. A specific case was discussed in [1]. Suppose we have a hybrid quantum code wherein  $d$  qubit codes  $|\psi_j\rangle$ ,  $1 \leq j \leq d$ , are each labelled by a classical “address”  $|j\rangle$ ,  $1 \leq j \leq d$ . In this case  $P = \sum_{j=1}^d \mathbf{1}_2 \otimes |j\rangle\langle j| = \mathbf{1}_2 \otimes \mathbf{1}_d$  and the algebra is  $\mathcal{A} = \oplus_{j=1}^d \mathcal{L}(\mathbf{C}^2) \otimes |j\rangle\langle j|$ . A generic density operator for this code is of the form  $\rho = \sum_{j=1}^d \alpha_j \rho_j \otimes |j\rangle\langle j|$ , where  $\rho_j = |\psi_j\rangle\langle\psi_j|$ ,  $\alpha_j \geq 0$ , and  $\sum_{j=1}^d \alpha_j = 1$ . This hybrid code determined by  $\mathcal{A}$  and  $P$  is correctable for  $\mathcal{E}$  if and only if for all  $a, b, j$  there are scalars  $\lambda_{abj}$  such that

$$PE_a^\dagger E_b P = \sum_{j=1}^d \lambda_{abj} (\mathbf{1}_2 \otimes |j\rangle\langle j|).$$

As the ancilla for each individual qubit  $|\psi_j\rangle$  is one-dimensional, in this case the correction operation will correct the code precisely,  $(\mathcal{R} \circ \mathcal{E})(\rho) = \rho$ .

In the Schrödinger picture, the correction channel built in the proofs of Theorems 9 and 11 is equal to

$$\mathcal{R}(\rho) = \sum_k \mathcal{R}_k(Q_k \rho Q_k) + \frac{\text{Tr}(Q^\perp \rho)}{\text{Tr} P} P,$$

In words, one first measures the observable defined by the complete set of orthogonal projectors  $Q_k$  and  $Q^\perp$ . If the state is found to be in one of the subspaces  $Q_k$  then the OQEC correction channel  $\mathcal{R}_k$  is applied to correct the corresponding subsystem of the algebra. Otherwise, if the state happens to be in the subspace  $Q^\perp$ , this means that the initial state of the system was not in the code. Therefore what we do in this case does not matter. In the channel  $\mathcal{R}$  defined above, we chose for simplicity to set the state to  $P/\text{Tr} P$ .

#### IV. APPLICATION TO INFORMATION FLOW

Consider the interaction between a “system”  $S$  and an “apparatus”  $A$  where the initial state of the apparatus is known. For any state  $|\psi_S\rangle \in \mathcal{H}_S$ , we define  $V|\psi_S\rangle \doteq U(|\psi_S\rangle \otimes |\psi_A\rangle)$

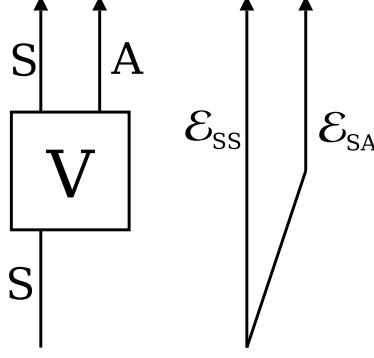


FIG. 1: Interaction between a system  $S$  and an apparatus  $A$  of known initial state. Tracing over one of the two final system gives us one of two channels  $\mathcal{E}_{SS}$  or  $\mathcal{E}_{SA}$ .

for a unitary  $U$  acting on  $\mathcal{H}_S \otimes \mathcal{H}_A$  and a fixed initial state  $|\psi_A\rangle \in \mathcal{H}_A$ . The operator  $V$  is an isometry between the space  $\mathcal{H}_S$  and the space  $\mathcal{H}_S \otimes \mathcal{H}_A$ . Tracing over the final state of the apparatus gives us a channel from  $B(\mathcal{H}_S)$  to  $B(\mathcal{H}_S)$ :  $\mathcal{E}_{SS}(\rho) = \text{Tr}_A(V\rho V^\dagger)$  whose dual is

$$\mathcal{E}_{SS}^\dagger(X) = V^\dagger(X \otimes \mathbf{1})V$$

We can also trace out the final state of the system to get a channel from  $\mathcal{L}(\mathcal{H}_S)$  to  $\mathcal{L}(\mathcal{H}_A)$ :  $\mathcal{E}_{SA}(\rho) = \text{Tr}_S(V\rho V^\dagger)$  where  $\rho \in B(\mathcal{H}_S)$ . See Figure 1. The channel  $\mathcal{E}_{SA}$  is uniquely defined by  $\mathcal{E}_{SS}$ , up to an arbitrary unitary operation on the apparatus, and is usually called the *complementary channel* of  $\mathcal{E}_{SS}$ . Its dual is simply

$$\mathcal{E}_{SA}^\dagger(Y) = V^\dagger(\mathbf{1} \otimes Y)V.$$

Using Theorem 9, we can determine which observables have been preserved by either  $\mathcal{E}_{SS}$  or  $\mathcal{E}_{SA}$ , irrespectively of the system's initial state. The answers are given by two subalgebras of  $\mathcal{L}(\mathcal{H}_S)$ : respectively  $\mathcal{A}_{SS}$  and  $\mathcal{A}_{SA}$ . The algebra  $\mathcal{A}_{SS}$  characterizes the information about the system's initial state which has been preserved by the system's evolution, and  $\mathcal{A}_{SA}$  characterizes the information about the system's initial state which has been transferred to the environment.

Those algebras can be expressed in terms of the elements of one of the channels. For instance, if  $E_a$  are elements for  $\mathcal{E}_{SS}$ , then  $V$  can be expressed as  $V = \sum_b E_b \otimes |\phi_b^A\rangle$  for some orthonormal set of vectors  $|\phi_b^A\rangle$  of  $\mathcal{H}_A$ . Hence for any choice of a basis  $|a\rangle$  of  $\mathcal{H}_S$  we obtain

a family of elements for the channel  $\mathcal{E}_{SA}$ , namely

$$F_a = \sum_b |\phi_b^A\rangle\langle a|E_b.$$

This means that the relevant operators entering Theorem 9 for the second channel are

$$F_a^\dagger F_b = \sum_c E_c^\dagger |a\rangle\langle b|E_c = \mathcal{E}_{SS}^\dagger(|a\rangle\langle b|).$$

Note that the operators  $|a\rangle\langle b|$  form a basis for the whole operator algebra  $\mathcal{L}(\mathcal{H}_S)$ . Hence the observables correctable for the apparatus form the algebra  $\mathcal{A}_{SA} = \text{Alg}(\text{Ran } \mathcal{E}_{SS}^\dagger)'$ : the algebra of operators commuting with all operators in the range of  $\mathcal{E}_{SS}^\dagger$ . Hence we see that a direct consequence of Theorem 9 is that in an open dynamics defined by a channel  $\mathcal{E}$ , full information about a projective observable can escape the system if and only if it commutes with the range of the dual map  $\mathcal{E}^\dagger$ , which is the set of observables with first moment information conserved by  $\mathcal{E}$ . This generalizes results in [25].

We can characterize the observables representing information which has been “duplicated” between the system and the apparatus. They form the intersection

$$\mathcal{C} := \mathcal{A}_{SS} \cap \mathcal{A}_{SA}.$$

From the correctability of  $\mathcal{A}_{SS}$  (Eq. (7)) we have that  $\mathcal{A}_{SS} \subseteq \text{Ran } \mathcal{E}_{SS}^\dagger$ , from which it follows that  $\mathcal{A}_{SA} = \text{Alg}(\text{Ran } \mathcal{E}_{SS}^\dagger)' \subseteq \mathcal{A}'_{SS}$ . Hence, the algebra of duplicated observables is  $\mathcal{C} \subseteq \mathcal{A}'_{SS} \cap \mathcal{A}_{SS}$ , where  $\mathcal{A}'_{SS} \cap \mathcal{A}_{SS}$  is the center of  $\mathcal{A}_{SS}$ : those elements of the algebra which commute with all other elements. In particular, the duplicated algebra  $\mathcal{C}$  is *commutative*. Note that the contrary would have violated the no-cloning theorem after correction of both channels. Since the algebra  $\mathcal{C}$  is commutative, it is generated by a single projective observable which can be represented by a self-adjoint operator  $C$ .

Given that, after the interaction, both the system and the apparatus contain information about the same observable  $C$  on the initial state of the system, we may expect that they are correlated. Let  $P_i \in \mathcal{C}$  be the projectors on the eigenspaces of  $C$ . There exists a POVM with elements  $X_i$  on the system as well as a POVM  $Y_i$  on the apparatus such that

$$\mathcal{E}_{SS}^\dagger(X_i) = \mathcal{E}_{SA}^\dagger(Y_i) = P_i.$$

Note that if  $\mathcal{R}_{SS}$  and  $\mathcal{R}_{SA}$  are correction channels for  $\mathcal{E}_{SS}$  and respectively  $\mathcal{E}_{SA}$ , then  $X_i = \mathcal{R}_{SS}^\dagger(P_i)$  and  $Y_i = \mathcal{R}_{SA}^\dagger(P_i)$ .



We will show that the observables  $X_i$  and  $Y_i$  are correlated. First note that  $\text{Tr}(P_i P_k) = \delta_{ki}$ , which we can also write

$$\text{Tr}(P_i P_k) = \text{Tr}(P_i \mathcal{E}_{SS}^\dagger(X_k)) = \text{Tr}(P_i V^\dagger(X_k \otimes \mathbf{1})V) = \delta_{ki}$$

This means that when  $k \neq i$ ,  $(X_k \otimes \mathbf{1})VP_i = 0$ , which can be seen by expanding  $P_i$  in terms of eigenvectors. Also since  $\sum_k X_k = \mathbf{1}$ , then  $VP_i = (X_i \otimes \mathbf{1})VP_i$ . The same argument is true also for  $Y_k$ . Therefore  $(X_k \otimes \mathbf{1})VP_i = (\mathbf{1} \otimes Y_k)VP_i = \delta_{ik}VP_i$ . Hence

$$V^\dagger(X_i \otimes Y_j)V = \sum_{kl} P_k V^\dagger(X_i \otimes Y_j)VP_l = \sum_{kl} \delta_{ik} \delta_{jl} P_i P_j = \delta_{ij} P_i$$

which means that for any state  $\rho$  of the system

$$\text{Tr}(V\rho V^\dagger(X_i \otimes Y_j)) = \delta_{ij} \text{Tr}(\rho P_i).$$

Hence the probability that the outcome of a measurement of  $X$  differs from that of  $Y$  is zero. This means that the information that the apparatus “learns” about the system and which is characterized by the observable  $C$  is correlated with a property of the system after the interaction. Therefore  $C$  represents the only information that the apparatus acquires about the system and which stays pertinent through the interaction.

This analysis has implication for the theory of decoherence [29, 30] as well as for the theory of measurements. We have shown that any interaction between a system and its environment (which took the role of the apparatus) automatically selects a unique observable  $C$  as being the only *predictive* information about the system acquired by the environment. Even though an observer who has access to the environment could learn about any observable contained in the algebra  $\mathcal{A}_{SA}$ , only the information encoded by  $C$  bears any information about the future state of the system. This suggests that the pointer states which characterize decoherence should not be selected only for their stability under the interaction with the environment: One should also add the requirement that they encode information that the environment learns about the system. Indeed any one of those requirements taken separately does not select a single observable unambiguously, but together they do. This is a new way of solving the *basis ambiguity* problem [31].

## V. ERROR CORRECTION OF OPERATOR SPACES

In this section we discuss an extension of OAQEC theory to the setting of operator spaces generated by observables. We shall leave a deeper analysis of this extension for investigation elsewhere. An *operator space* [32] is a linear manifold (a subspace) of operators inside  $\mathcal{L}(\mathcal{H})$ . Operator spaces, and their Hermitian closed counterpart “operator systems”, have arisen recently in the study of channel capacity problems in quantum information [33]. Observe that (by design) Definitions 3 and 8 include the case of operator spaces and systems generated by observables, and hence these cases fit into the mathematical framework for error correction introduced here. Let us describe how operator spaces physically arise in the present setting.

In Section III A we showed how to build the correction channel for active error correction. We were free to choose what to do to the system in the case that the syndrome measurement revealed the state had not initially been in the code prior to the action of the error channel. In fact, there is an advantage in choosing to send that state back in the code, meaning that we choose the correction channel such that  $\mathcal{R}^\dagger(X) = \mathcal{R}^\dagger(PXP)$  for any operator  $X$ , which is indeed the case for the correction channel defined in Theorem 11. Consider the set of operators defined by

$$\mathcal{V} := \mathcal{E}^\dagger(\mathcal{R}^\dagger(\mathcal{A})).$$

This set is not an algebra in general. Nevertheless, it is an operator system by the linearity and positivity of channels. If  $X \in \mathcal{V}$  then there exists  $Y \in P\mathcal{A}P$  such that  $X = \mathcal{E}^\dagger(\mathcal{R}^\dagger(Y))$  and also  $PXP = Y$ . Therefore for all  $X \in \mathcal{V}$ ,

$$\mathcal{E}^\dagger(\mathcal{R}^\dagger(X)) = \mathcal{E}^\dagger(\mathcal{R}^\dagger(Y)) = X.$$

Hence the observables in  $\mathcal{V}$  are exactly corrected, and this is *independent* of what the initial state was. For instance, if we “forgot” to make sure that the initial state was in the code, we can still recover all the information, provided that we measure the observable with elements  $X_k = \mathcal{E}^\dagger(\mathcal{R}^\dagger(Y_k))$  whenever we would have measured  $Y_k \in \mathcal{A}$ . Typically this would involve measuring general (unsharp) POVMs instead of just sharp projective observables. This shows that it could be useful to consider the correction of general POVMs. Since POVM elements do not always span an algebra, this suggests that we should consider the correctability (passive or active) codes associated with operator systems in this way.

Consider the following simple example of a conserved operator space that is not an algebra. Let  $\mathcal{H}$  be single qutrit Hilbert space with computational basis  $\{|0\rangle, |1\rangle, |2\rangle\}$ . Consider the channel  $\mathcal{E}$  on  $\mathcal{H}$  defined by its action on observables represented in this basis as follows:

$$\mathcal{E}^\dagger\left([a_{ij}]_{3 \times 3}\right) = \begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & \frac{a_{11}+a_{22}}{2} \end{bmatrix}. \quad (12)$$

Observe that  $(\mathcal{E}^\dagger)^2 = \mathcal{E}^\dagger \circ \mathcal{E}^\dagger = \mathcal{E}^\dagger$  and that the range  $\mathcal{V}$  of  $\mathcal{E}^\dagger$  coincides with its fixed point set;  $\{Y : Y = \mathcal{E}^\dagger(X) \text{ for some } X\} = \{X : \mathcal{E}^\dagger(X) = X\}$ . Thus, the operator system  $\mathcal{V}$  is conserved by  $\mathcal{E}$ . Moreover,  $\mathcal{V}$  is not an algebra since it is not closed under multiplication.

Given results from other settings for quantum error correction, it is of course desirable to find a characterization of correction for operator spaces independent of any particular recovery operation. Here we derive a necessary condition, and we leave the general question as an open problem. Observe that if there exists a channel  $\mathcal{R}$  such that  $P\mathcal{E}^\dagger(\mathcal{R}^\dagger(X))P = PXP$  for all  $X \in \mathcal{V}$  then,  $0 \leq X \leq \mathbf{1}$  implies  $0 \leq \mathcal{R}^\dagger(X) \leq \mathbf{1}$ , since  $\mathcal{R}^\dagger$  is a contractive map. This in turn implies that there exists  $0 \leq Y \leq \mathbf{1}$  such that  $PXP = P\mathcal{E}^\dagger(Y)P$ ; namely,  $Y = \mathcal{R}^\dagger(X)$ .

**Proposition 12.** *A necessary condition for an operator space  $\mathcal{V}$  to be correctable on states  $P\mathcal{H}$  for  $\mathcal{E}$  is that for all  $X \in \mathcal{V}$  such that  $0 \leq X \leq \mathbf{1}$ , there exists  $0 \leq Y \leq \mathbf{1}$  such that  $PXP = P\mathcal{E}^\dagger(Y)P$ . This condition is also sufficient when  $\mathcal{V}$  is an algebra containing  $P$ .*

**Proof.** The first part of the statement has been proved. We show that the condition expressed implies correctability of  $\mathcal{V}$  if it is an algebra containing  $P$ .

Since  $P \in \mathcal{V}$ , we know that  $\mathcal{B} := P\mathcal{V}P$  is a subalgebra of  $\mathcal{V}$ . Note it is sufficient to prove the correctability of  $\mathcal{B}$ . Indeed, if  $\mathcal{B}$  is correctable then in particular  $P$  is correctable. Let  $\mathcal{R}$  be a correction channel for the largest correctable algebra on  $P\mathcal{H}$ . Then we have seen in the proof of Theorem 11 that the correctability of  $P$  implies that  $P\mathcal{E}^\dagger(\mathcal{R}^\dagger(X))P = P\mathcal{E}^\dagger(\mathcal{R}^\dagger(PXP))P$  for any  $X$ . From this it follows that the correctability of  $\mathcal{B}$  on  $P\mathcal{H}$  implies that of  $\mathcal{V}$ .

Let  $\mathbb{E} := \{X \mid 0 \leq X \leq \mathbf{1}\}$ . Suppose that  $P(V \cap \mathbb{E})P = \mathcal{B} \cap \mathbb{E} \subseteq P\mathcal{E}^\dagger(\mathbb{E})P$ . Then for all projectors  $Q \in \mathcal{B}$ , there exists a self-adjoint operator  $0 \leq X \leq \mathbf{1}$  such that  $P\mathcal{E}^\dagger(X)P = Q$ .

Hence  $(P - Q)\mathcal{E}^\dagger(X)(P - Q) = 0$ , which implies  $XE_k(P - Q) = 0$ , or  $XE_kP = XE_kQ$  for all  $k$ . Also we have  $P\mathcal{E}^\dagger(\mathbf{1} - X)P = P - Q$ , so that  $Q\mathcal{E}^\dagger(\mathbf{1} - X)Q = 0$  from which  $(\mathbf{1} - X)E_kQ = 0$ , or  $E_kQ = XE_kQ$  for all  $k$ . Therefore

$$X(E_kP) = XE_kQ = E_kQ = (E_kP)Q.$$

Combining the two results we obtain

$$QPE_k^\dagger E_jP = PE_k^\dagger XE_jP = PE_k^\dagger E_jPQ$$

for all  $k$  and all  $j$ . This result can linearly be extended to the whole of  $\mathcal{B}$ , since an algebra is spanned by its projectors. Hence  $[X, PE_k^\dagger E_jP] = 0$  for all  $X \in \mathcal{B}$ . From Theorem 11 this implies that  $\mathcal{B}$ , and therefore the algebra  $\mathcal{V}$  is correctable on  $P\mathcal{H}$ .  $\square$

As a final example, consider the noise model corresponding to a single random bit flip on three qubits. The noise operators are  $\{\mathbf{1}, X_1, X_2, X_3\}$  where  $X_i$  is a Pauli  $x$  matrix on the  $i$ th qubit. One can correct the standard quantum code with projector  $P = |000\rangle\langle 000| + |111\rangle\langle 111|$  expressed in the computational basis. It is easy to check that a correction channel for this code is

$$\mathcal{R}^\dagger(A) = PAP + \sum_i X_i PAPX_i$$

This channel has the properties that we need in order to “lift” the code to an operator space code correctable on all states. Indeed, we have  $\mathcal{R}^\dagger(P) = \mathbf{1}$  and  $\mathcal{R}^\dagger(A) = \mathcal{R}^\dagger(PAP)$  for all  $A$ . The algebra correctable on the code  $P$  is

$$\mathcal{A} = \left\{ \sum_{ij} \alpha_{ij} |iii\rangle\langle jjj| : \alpha_{ij} \in \mathbb{C} \right\}$$

In order to proceed however we need a specific error channel, which is given by choosing a probability for the occurrence of each error:

$$\mathcal{E}(\rho) = p_0\rho + \sum_i p_i X_i \rho X_i$$

Then, writing  $X_0 = \mathbf{1}$ , the operator space

$$\mathcal{V} = (\mathcal{R} \circ \mathcal{E})^\dagger(\mathcal{A}) = \left\{ \sum_{i,j=0}^1 \alpha_{ij} \sum_{k,l=0}^3 p_k X_k X_l |iii\rangle\langle jjj| X_l X_k : \alpha_{ij} \in \mathbb{C} \right\}$$

is correctable by  $\mathcal{R}$  on all states. We should have  $P\mathcal{V}P = \mathcal{A}$ . This can be seen from the fact that  $|iii\rangle = P|iii\rangle$  and  $PX_kX_lP = \delta_{kl}P$ . Explicitly separating the components respectively inside  $\mathcal{A}$  and orthogonal to  $\mathcal{A}$  we have operators in  $\mathcal{V}$  which live in  $\mathcal{A}$  and outside of  $\mathcal{A}$ :

$$\mathcal{V} = \left\{ \sum_{ij} \alpha_{ij} \left( |iii\rangle\langle jjj| + \sum_{k \neq l} p_k X_k X_l |iii\rangle\langle jjj| X_l X_k \right) : \alpha_{ij} \in \mathbb{C} \right\}$$

*Acknowledgements.* We are grateful to the Banff International Research Station for kind hospitality. Some of the work for this paper took place during workshop 07w5119 on “Operator structures in quantum information theory”. This work was partially supported by NSERC, PREA, ERA, CFI, OIT, and the Canada Research Chairs program.

- 
- [1] C. Bény, A. Kempf, and D. W. Kribs, Phys. Rev. Lett., **98**, 100502 (2007).
  - [2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
  - [3] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
  - [4] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
  - [5] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
  - [6] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
  - [7] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
  - [8] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, Quant. Inf. & Comp. **6**, 382 (2006).
  - [9] G. Kuperberg, IEEE Trans. Inform. Theory **49**, 1465 (2003).
  - [10] M. A. Nielsen, and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press (2000).
  - [11] J. von Neumann, *Mathematical foundations of quantum mechanics*, Princeton University Press, Princeton, 1955.
  - [12] K. R. Davidson, *C\*-algebras by example*, Fields Institute Monographs, 6. American Mathematical Society, Providence, RI, 1996.
  - [13] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
  - [14] G. Palma, K.-A. Suominen, and A. Ekert, Proc. Royal Soc. A **452**, 567 (1996).
  - [15] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
  - [16] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

- [17] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
- [18] P. Zanardi, Phys. Rev. A **63**, 12301 (2001).
- [19] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 42307 (2001).
- [20] M. Junge, P. Kim, and D. W. Kribs, J. Math. Phys. **46**, 022102 (2005).
- [21] J.A. Holbrook, D.W. Kribs, R. Laflamme, and D. Poulin, Integral Eqtns. & Operator Thy., **51** (2005), 215-234.
- [22] J.A. Holbrook, D.W. Kribs, and R. Laflamme, Quant. Inf. Proc. **2**, (2004), 381-419.
- [23] M.-D. Choi and D. W. Kribs, Phys. Rev. Lett. **96**, 050501 (2006).
- [24] E. Knill, e-print quant-ph/0603252 (2006).
- [25] G. Lindblad, Lett. Math. Phys. **47**, 189 (1999).
- [26] D. W. Kribs, Proc. Edin. Math. Soc. **46**, 421 (2003).
- [27] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, W. H. Zurek, LA Science **27**, 188 (2002).
- [28] M. A. Nielsen and D. Poulin, e-print quant-ph/0506069 (2005).
- [29] D. Giulini *et al.*, *Decoherence and the Appearance of a Classical World in Quantum Theory* (Springer, Berlin, 1996).
- [30] W. H. Zurek, Rev. Mod. Phys. **75**, 715 (2003).
- [31] W. H. Zurek, Phys. Rev. D **24**, 1516 (1981).
- [32] V. Paulsen, *Completely bounded maps and operator algebras*, Cambridge University Press, Cambridge, United Kingdom, 2002.
- [33] I. Devetak, M. Junge, C. King, and M. B. Ruskai, Comm. Math. Phys., **266** (2006), 37-63.